

Software Assurance Program Working Groups

The Department of Homeland Security (DHS) National Cyber Security Division's (NCSD) Software Assurance Program directly supports the President's goals for securing cyberspace, as articulated in Priority II of the National Strategy to Secure Cyberspace, dated February 2003. Consistent with HSPD-7, NCSD serves as a focal point for software assurance, as part of ensuring the security of cyberspace, and works closely with the private sector, academia, and other government agencies to improve software development processes that will lead to the production of better quality and more secure software in support of mission assurance. NCSD's Software Assurance Program is targeted on the following four areas:

- **People** – developers and users (includes education and training)
- **Processes** – best practices and practical guidelines for the development of secure software; standards
- **Technology** – software evaluation tools and security technology
- **Acquisition** – software security improvements through acquisition specifications and guidelines

NCSD has established stakeholder working groups to support each of the program areas. The goal of the working groups is to continue to support the Software Assurance initiatives by bringing together members of government, industry, and academia with vested interests in software security, to discuss and promulgate applicable practices and methodologies. There are currently four working groups underway:

Software Common Body of Knowledge – Focuses on the People aspect of Software Assurance. The goal of this working group is to develop a Software Assurance Common Body of Knowledge from which to develop curriculum for universities. The CBK is planned to be released in October and finalized in December 2005, with a pilot occurring next year.

Software Processes and Practices – Focuses on the Process aspect of Software Assurance. The goal of this group is to specifically look at how process guidance, standards, practice examples, configuration guidance, and conformance checks can best help promote software assurance.

Software Technology, Tools, and Product Evaluation – Focuses on the Technology aspect of Software Assurance. This working group will look at product evaluations and related tools and discuss best ways to facilitate research. It will also look at the Federated Lab vision and provide a vision and develop a Concept of Operations for a malicious code/tools and technique repository.

Software Acquisition – Focuses on the Acquisition aspect of Software Assurance. This working group will look at enhancing software supply chain management through improved risk mitigation and contracting for secure software.

In order to request to participate in the Software Assurance working groups, please visit the US-CERT portal (<https://us-cert.esportals.net/>) and register with the organization ID 223. After registering, you will receive a follow-up on joining a working group.